



VIRGINIA ALCOHOLIC BEVERAGE CONTROL AUTHORITY

REPORT ON AUDIT FOR THE YEAR ENDED JUNE 30, 2023

Auditor of Public Accounts
Staci A. Henshaw, CPA

www.apa.virginia.gov

(804) 225-3350



AUDIT SUMMARY

We have audited the basic financial statements of the Virginia Alcoholic Beverage Control Authority (Authority) as of and for the year ended June 30, 2023, and issued our report thereon, dated December 12, 2023. Our report is included in the Authority's Annual Report that it anticipates releasing in December 2023.

Our audit of the Authority found:

- the financial statements are presented fairly, in all material respects;
- three internal control findings requiring management's attention; however, we do not consider them to be material weaknesses; and
- two instances of noncompliance or other matters required to be reported under Government Auditing Standards.

In the section titled "Internal Control and Compliance Findings and Recommendations" we have included our assessment of the conditions and causes resulting in the internal control and compliance findings identified through our audits as well as recommendations for addressing those findings. Our assessment does not remove management's responsibility to perform a thorough assessment of the conditions and causes of the findings and developing and appropriately implementing adequate corrective actions to resolve the findings as required by the Department of Accounts in Section 10205 – Agency Response to APA Audit of the Commonwealth Accounting Policies and Procedures Manual. Those corrective actions may include additional items beyond our recommendations.

–TABLE OF CONTENTS–

Pages

AUDIT SUMMARY

INTERNAL CONTROL AND COMPLIANCE FINDINGS AND RECOMMENDATIONS

1-4

INDEPENDENT AUDITOR’S REPORT ON INTERNAL CONTROL OVER
FINANCIAL REPORTING AND ON COMPLIANCE AND OTHER MATTERS

5-7

AUTHORITY RESPONSE

8-9

APPENDIX – FINDINGS SUMMARY

10

INTERNAL CONTROL AND COMPLIANCE FINDINGS AND RECOMMENDATIONS

Improve IT Risk Management and Contingency Planning

Type: Internal Control and Compliance

Severity: Significant Deficiency

The Alcoholic Beverage Control Authority (Authority) does not manage its information technology (IT) risk management and contingency planning program in accordance with its Information Security Risk Management Policy (Risk Management Policy), its Information Security Policy (Security Policy), and its adopted information security standard, the National Institute of Standards and Technology Standard, 800-53 (NIST Standard). Specifically, the following weaknesses exist:

- The Authority does not annually update its IT Systems and Data Sensitivity Classification as part of its business impact analysis process. By not having an updated Data Sensitivity Classification to classify current systems based on sensitivity according to an analysis based on the confidentiality, integrity, and availability of the data, the Authority increases the risk for an inaccurate classification of systems. This may lead to the Authority not implementing the necessary security controls for its systems and IT environment (*Security Policy, Section: 3.3.5.3.1.a IT Contingency Planning; NIST Standard, Section: RA-2 Security Categorization*).
- The Authority does not have a completed risk assessment on record for six of its 16 (38%) sensitive systems. The Risk Management Policy requires the Authority to conduct a risk assessment for critical information systems and critical production applications at least once every three years. Without completing risk assessments for each sensitive system, the Authority may not identify potential risks in their sensitive systems, which increases the risk of not having mitigating controls in place to prevent a compromise of its sensitive data (*Risk Management Policy, Section: 2.c Information System Security Risk Assessment; Security Policy, Section: 2.2.3 Infosec Program Activities Inputs and Outputs; NIST Standard, Section: RA-3 Risk Assessment*).
- The Authority does not have a system security plan (SSP) for any of its 16 sensitive systems. The Security Policy requires the Authority to complete an SSP for all sensitive IT systems and perform an annual review for updates. Not having an SSP for each sensitive system could result in the Authority not properly identifying risks and mitigating controls for each sensitive system (*Security Policy, Section: 3.3.10.3.2.a Application/System Development Life Cycle Security; NIST Standard, Section: PL-2 System Security and Privacy Plans*).
- The Authority does not test its Continuity of Operations Plan (COOP) annually in accordance with its testing strategy. The Authority last performed a test of its COOP in the calendar year 2020. The NIST Standard requires the Authority to test the contingency plan to determine the effectiveness of the plan and readiness to execute the plan. Not regularly testing the COOP could result in the Authority's inability to execute the COOP successfully when needed

to support the contingency procedures and ensure IT resources are operational (*NIST Standard, Section: CP-4 Contingency Plan Testing; COOP, Section: Training and Exercises*).

- The Authority does not document and execute a strategy for disaster recovery testing that includes testing IT components of the Authority's Disaster Recovery Plan (DRP). The NIST Standard requires the Authority to test the effectiveness of incident response capabilities for systems and coordinating incident response testing with elements responsible for related plans, such as the COOP and DRP (*NIST Standard, Sections: IR-3 Incident Response Testing, CP-4 Contingency Plan Testing, CP-9 CE2 System Backup: Test Restoration Using Sampling*).

Limited resources and staffing turnover in the IT department resulted in the weaknesses identified above. The Authority hired a new Information Security Officer (ISO) in June 2022. In fiscal year 2023 the ISO began reviewing and updating the Authority's policies and procedures, as well as updating and completing the IT risk management artifacts, including risk assessments, SSPs, and the data sensitivity classifications.

The Authority should dedicate the necessary resources to review and revise its Data Sensitivity Classification to ensure its systems' sensitivity classification is accurate. The Authority should also conduct or update its risk assessments and SSPs for all sensitive systems. Additionally, the Authority should perform annual reviews of the Data Sensitivity Classification, risk assessments, and SSPs to ensure all documents remain current. The Authority should document a formal strategy for disaster recovery testing and execute its COOP and DRP testing strategies on an annual basis to ensure it can perform manual processes and restore essential functions within the defined recovery timeframes. This will help ensure the Authority protects the confidentiality, integrity, and availability of its sensitive and mission critical systems and data.

Continue Improving Oversight of Third-Party Service Providers

Type: Internal Control and Compliance

Severity: Significant Deficiency

First Issued: Fiscal Year 2020

The Authority has made significant progress to develop a formal and consistent process to oversee and manage its IT third-party service providers (providers) in accordance with the NIST Standard. Providers are entities that perform tasks and business functions on behalf of the Authority.

Since the prior year's audit, the Authority has revised its Procurement Policy and developed procedures that establish a formal process to procure and monitor its providers on an ongoing basis. However, the following two weaknesses remain:

- The Authority has not received and reviewed independent audit assurance for five of its 46 (11%) providers. The Authority's procedures require the Information Security Department, or functional area responsible for reviews, to obtain and review a System and Organization Controls (SOC) report. By not receiving and reviewing independent audit assurance, such as a SOC report, for each provider on an ongoing basis, the Authority cannot validate that the

providers have effective IT controls to protect the Authority's sensitive and confidential data, increasing the chance of a breach or possible data disclosure.

- The Authority has not completed a formal risk assessment for 43 of its 46 (93%) providers. The Authority's Information Security Risk Management Policy requires the Information Security department to perform information systems security risk assessments for critical information systems and production applications at least once every three years. Without completing risk assessments, the Information Security department is unable to determine the risks that impact the Authority's sensitive data or providers and dedicate the resources to implement appropriate security controls to reduce or mitigate those risks.

During fiscal year 2023 the ISO developed and implemented a new provider oversight process. Due to the timing of the Authority's implementation of the new process, the Authority did not have sufficient time to complete its corrective actions to fully resolve the prior year's weaknesses.

The Authority should continue enforcing its new policy and procedure to obtain and review independent audit assurance for each provider on an ongoing basis. The Authority should also conduct a formal risk assessment for each provider to validate IT controls and mitigate potential risks. This will help to safeguard the confidentiality, integrity, and availability of the Authority's sensitive and mission critical data.

Improve Internal Controls over Employee Separation Process

Type: Internal Control

Severity: Significant Deficiency

First Issued: Fiscal Year 2022

The Authority does not have adequate internal controls over the completion of off-boarding checklists or removing access for terminated employees. Our sample of 30 terminated employees during fiscal year 2023 found:

- Supervisors completed eight of 30 (27%) checklists six to 34 business days after the employees' termination date; and
- For eight of 30 (27%) employees, the Authority removed system access six to 48 business days after the employees' termination date. Six instances were related to the Authority's active directory and two instances were related to the Commonwealth's electronic procurement system.

The Authority's human resource system generates an off-boarding checklist with multiple sections for completion by various departments. The five-day timeframe within the Authority's separations procedures is specific to the section of the checklist the direct supervisor must complete. The policy does not define specific timeframes for the completion of the other sections, which includes human resources, payroll, and information systems, nor does it define a timeframe for system removal. This makes it difficult to enforce adherence to policy and ensure timeliness of completion.

The Authority relies on active directory for the management of access to many of the Authority's critical systems, including the financial management system and the inventory and logistics system. Therefore, Human Resources does not track the removal of system access outside of the Authority's active directory. This leaves systems outside of the Authority's active directory, such as the Commonwealth's statewide systems, at risk for not having access removed timely.

A critical function of completed checklists is to ensure the timely removal of access to the Authority's systems and return of property. The Authority should review their current termination practices to ensure their policy is reasonable and effective internal controls are in place. Additionally, due to the Authority's unique structure, the Authority should define specific procedures for retail store employees, enforcement employees, and headquarter employees as access levels and risks are inherently different. This will enable Human Resources to better monitor and hold supervisors accountable for the timely completion of employee checklists and access removal.



Staci A. Henshaw, CPA
Auditor of Public Accounts

Commonwealth of Virginia

Auditor of Public Accounts

P.O. Box 1295
Richmond, Virginia 23218

December 12, 2023

The Honorable Glenn Youngkin
Governor of Virginia

Joint Legislative Audit
and Review Commission

Virginia ABC Board of Directors
Virginia Alcoholic Beverage Control Authority

Thomas Kirby, Interim CEO
Virginia Alcoholic Beverage Control Authority

INDEPENDENT AUDITOR'S REPORT ON INTERNAL CONTROL OVER FINANCIAL REPORTING AND ON COMPLIANCE AND OTHER MATTERS

We have audited, in accordance with the auditing standards generally accepted in the United States of America and the standards applicable to financial audits contained in Government Auditing Standards, issued by the Comptroller General of the United States, the financial statements of the **Virginia Alcoholic Beverage Control Authority** (Authority) as of and for the year ended June 30, 2023, and the related notes to the financial statements, which collectively comprise the Authority's basic financial statements, and have issued our report thereon dated December 12, 2023.

Internal Control Over Financial Reporting

In planning and performing our audit of the financial statements, we considered the Authority's internal control over financial reporting (internal control) as a basis for designing audit procedures that are appropriate in the circumstances for the purpose of expressing our opinion on the financial statements, but not for the purpose of expressing an opinion on the effectiveness of the Authority's internal control. Accordingly, we do not express an opinion on the effectiveness of the Authority's internal control.

A deficiency in internal control exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent, or detect and correct, misstatements on a timely basis. A material weakness is a deficiency, or a combination of deficiencies, in internal control, such that there is a reasonable possibility that a material misstatement of the entity's financial statements will not be prevented, or detected and corrected, on a timely basis. A significant deficiency is a deficiency, or a combination of deficiencies, in internal control that is less severe than a material weakness, yet important enough to merit attention by those charged with governance.

Our consideration of internal control was for the limited purpose described in the first paragraph of this section and was not designed to identify all deficiencies in internal control that might be material weaknesses or significant deficiencies and, therefore, material weaknesses or significant deficiencies may exist that were not identified. Given these limitations, during our audit we did not identify any deficiencies in internal control that we consider to be material weaknesses. We did identify certain deficiencies in internal control titled “Improve IT Risk Management and Contingency Planning,” “Continue Improving Oversight of Third-Party Service Providers,” and “Improve Internal Controls over Employee Separation Process,” which are described in the section titled “Internal Control and Compliance Findings and Recommendations,” that we consider to be significant deficiencies.

Compliance and Other Matters

As part of obtaining reasonable assurance about whether the Authority’s financial statements are free of material misstatement, we performed tests of its compliance with certain provisions of laws, regulations, contracts, and grant agreements, noncompliance with which could have a direct and material effect on the financial statements. However, providing an opinion on compliance with those provisions was not an objective of our audit and, accordingly, we do not express such an opinion. The results of our tests disclosed instances of noncompliance or other matters that is required to be reported under Government Auditing Standards and which are described in the section titled “Internal Control and Compliance Findings and Recommendations” in the findings titled “Improve IT Risk Management and Contingency Planning,” and “Continue Improving Oversight of Third-Party Service Providers.”

The Authority’s Response to Findings

We discussed this report with management at an exit conference held on December 11, 2023. Government Auditing Standards require the auditor to perform limited procedures on the Authority’s response to the findings identified in our audit, which is included in the accompanying section titled “Authority Response.” The Authority’s response was not subjected to the other auditing procedures applied in the audit of the financial statements and, accordingly, we express no opinion on the response.

Status of Prior Findings

The Authority has not taken adequate corrective action with respect to the prior reported findings identified as ongoing in the Findings Summary included in the Appendix. The Authority has taken adequate corrective action with respect to prior audit findings identified as complete in the Findings Summary included in the Appendix.

Purpose of this Report

The purpose of this report is solely to describe the scope of our testing of internal control and compliance and the results of that testing, and not to provide an opinion on the effectiveness of the entity's internal control or on compliance. This report is an integral part of an audit performed in accordance with Government Auditing Standards in considering the entity's internal control and compliance. Accordingly, this communication is not suitable for any other purpose.

Staci A. Henshaw
AUDITOR OF PUBLIC ACCOUNTS

JMR/clj

Virginia Alcoholic Beverage Control Authority

Interim Chief Executive Officer
Thomas W. Kirby



Chair
Timothy D. Hugo

Vice Chair
Robert C. Sledd

Board of Directors
William D. Euille
Gregory F. Holland
Mark E. Rubin

December 12, 2023

Ms. Staci A. Henshaw, CPA
Auditor of Public Accounts
101 N. 14th Street
Richmond, VA 23219

Dear Ms. Henshaw,

Attached are the Virginia Alcoholic Beverage Control Authority (“VA ABC,” the “Authority”) responses to the audit for fiscal year ended June 30, 2023. The Authority appreciates the opportunity to respond to the findings noted, and to strengthen our controls based on the recommendations. Our responses to the findings in the Report on Internal Controls follow.

Improve IT Risk Management and Contingency Planning

The Authority agrees with the findings. The noted findings are mostly about a backlog and timely update in VA ABC’s process documentation, largely caused by staff turnover. As most of VA ABC’s critical systems are relatively new and were fully assessed during acquisition and implementation, IT will work with Infosec to schedule systems review during the next fiscal year to reduce the backlog.

VA ABC’s systems are now mostly separate components that can operate independently. During the year, many of these presented challenges, but VA ABC successfully recovered these systems as part of its routine system support. We will work with Infosec for a documentation standard to meet the requirement for documenting testing of component results within the IT systems portfolio and conduct simulated tests of critical systems where there have been no exceptions to document. The Enforcement division is also planning a tabletop business continuity exercise this year in which IT will participate.



www.abc.virginia.gov | 7450 Freight Way Mechanicsville, VA 23116 | 804.213.4400

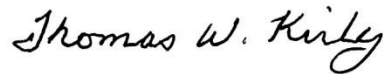
Continue Improving Oversight of Third-Party Service Providers

The Authority agrees with the finding. The Authority will request and review the System and Organization Controls (SOC) report for high risk, or sensitive systems, on an annual basis and will review the medium risk providers once every three years. Virginia ABC will also work with IT procurement to address the review of contracts to ensure that vendors are required to submit a SOC report.

Improve Internal Controls over Employee Separation Process

The Authority concurs with the exceptions noted and will enhance controls over employee separation process. The Authority will reassess our current processes and ensure all responsible leaders are following the guidelines related to the separation checklist. Furthermore, the Authority will provide additional training and support to the responsible leaders and will conduct quarterly audits to ensure compliance.

Sincerely,



Thomas W. Kirby
Interim Chief Executive Officer



www.abc.virginia.gov | 7450 Freight Way Mechanicsville, VA 23116 | 804.213.4400

FINDINGS SUMMARY

Finding Title	Status of Corrective Action	First Issued
Continue Improving Database Security	Complete	2019
Continue Improving Security Awareness and Training Program	Complete	2019
Continue Improving Oversight of Third-Party Service Providers	Ongoing	2020
Continue Improving Internal Controls over Employment Eligibility	Complete	2021
Continue Improving Internal Controls over Processing Payments	Complete	2021
Improve Internal Controls over Employee Separation Process	Ongoing	2022
Implement a Data/Records Retention Policy and Solution for Automated Reconciliations	Complete	2022
Retain Inventory Documentation	Complete	2022
Improve IT Risk Management and Contingency Planning	Ongoing	2023